

Contemporary Abstract Algebra

SEVENTH EDITION

Joseph A. Gallian
University of Minnesota Duluth

Definitions Greatest Common Divisor, Relatively Prime Integers

The *greatest common divisor* of two nonzero integers a and b is the largest of all common divisors of a and b . We denote this integer by $\gcd(a, b)$. When $\gcd(a, b) = 1$, we say a and b are *relatively prime*.

Definition Least Common Multiple

The least common multiple of two nonzero integers a and b is the smallest positive integer that is a multiple of both a and b . We will denote this integer by $\text{lcm}(a, b)$.

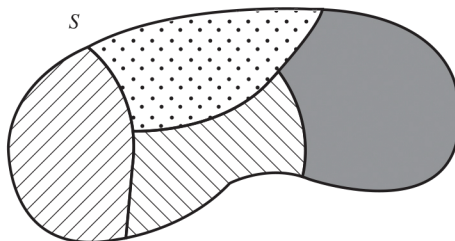
Definition Equivalence Relation

An *equivalence relation* on a set S is a set R of ordered pairs of elements of S such that

1. $(a, a) \in R$ for all $a \in S$ (reflexive property).
2. $(a, b) \in R$ implies $(b, a) \in R$ (symmetric property).
3. $(a, b) \in R$ and $(b, c) \in R$ imply $(a, c) \in R$ (transitive property).

Definition Partition

A *partition* of a set S is a collection of nonempty disjoint subsets of S whose union is S . The diagram illustrates a partition of a set into four subsets.



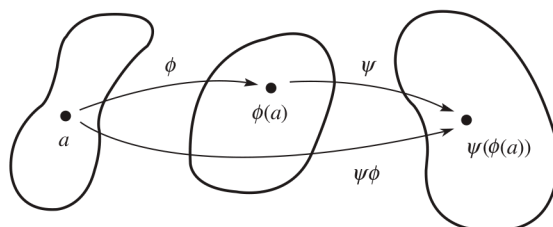
Partition of S into four subsets.

Definition Function (Mapping)

A *function* (or *mapping*) ϕ from a set A to a set B is a rule that assigns to each element a of A exactly one element b of B . The set A is called the *domain* of ϕ , and B is called the *range* of ϕ . If ϕ assigns b to a , then b is called the *image* of a under ϕ . The subset of B comprising all the images of elements of A is called the *image* of A under ϕ .

Definition Composition of Functions

Let $\phi: A \rightarrow B$ and $\psi: B \rightarrow C$. The *composition* $\psi\phi$ is the mapping from A to C defined by $(\psi\phi)(a) = \psi(\phi(a))$ for all a in A . The composition function $\psi\phi$ can be visualized as in Figure 0.6.



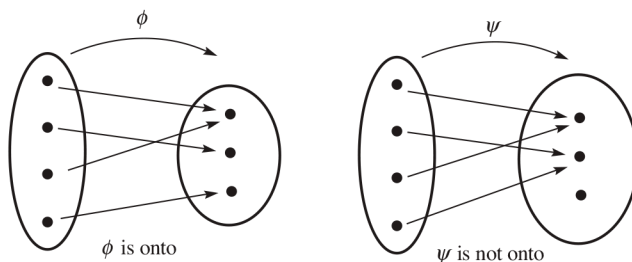
Composition of functions ϕ and ψ .

Definition One-to-One Function

A function ϕ from a set A is called *one-to-one* if for every $a_1, a_2 \in A$, $\phi(a_1) = \phi(a_2)$ implies $a_1 = a_2$.

Definition Function from A onto B

A function ϕ from a set A to a set B is said to be *onto* B if each element of B is the image of at least one element of A . In symbols, $\phi: A \rightarrow B$ is onto if for each b in B there is at least one a in A such that $\phi(a) = b$.



Definition Binary Operation

Let G be a set. A *binary operation* on G is a function that assigns each ordered pair of elements of G an element of G .

Definition Group

Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab . We say G is a *group* under this operation if the following three properties are satisfied.

1. *Associativity*. The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G .
2. *Identity*. There is an element e (called the *identity*) in G such that $ae = ea = a$ for all a in G .
3. *Inverses*. For each element a in G , there is an element b in G (called an *inverse* of a) such that $ab = ba = e$.

Definition Order of a Group

The number of elements of a group (finite or infinite) is called its *order*. We will use $|G|$ to denote the order of G .

Definition Order of an Element

The *order* of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would be $ng = 0$.) If no such integer exists, we say that g has *infinite order*. The order of an element g is denoted by $|g|$.

Definition Subgroup

If a subset H of a group G is itself a group under the operation of G , we say that H is a *subgroup* of G .

Definition Center of a Group

The *center*, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G . In symbols,

$$Z(G) = \{a \in G \mid ax = xa \text{ for all } x \text{ in } G\}.$$

[The notation $Z(G)$ comes from the fact that the German word for center is *Zentrum*. The term was coined by J. A. de Segurier in 1904.]

Definition Centralizer of a in G

Let a be a fixed element of a group G . The *centralizer of a in G* , $C(a)$, is the set of all elements in G that commute with a . In symbols, $C(a) = \{g \in G \mid ga = ag\}$.

Definitions Permutation of A , Permutation Group of A

A *permutation* of a set A is a function from A to A that is both one-to-one and onto. A *permutation group* of a set A is a set of permutations of A that forms a group under function composition.

Definition Even and Odd Permutations

A permutation that can be expressed as a product of an even number of 2-cycles is called an *even* permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an *odd* permutation.

Definition Alternating Group of Degree n

The group of even permutations of n symbols is denoted by A_n and is called the *alternating group of degree n* .

Definition Group Isomorphism

An *isomorphism* ϕ from a group G to a group $\bar{G}$ is a one-to-one mapping (or function) from G onto $\bar{G}$ that preserves the group operation. That is,

$$\phi(ab) = \phi(a)\phi(b) \quad \text{for all } a, b \text{ in } G.$$

If there is an isomorphism from G onto $\bar{G}$, we say that G and $\bar{G}$ are *isomorphic* and write $G \approx \bar{G}$.

Definition Automorphism

An isomorphism from a group G onto itself is called an *automorphism* of G .

Definition Inner Automorphism Induced by a

Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$ for all x in G is called the *inner automorphism of G induced by a* .

Definition Coset of H in G

Let G be a group and let H be a subset of G . For any $a \in G$, the set $\{ah \mid h \in H\}$ is denoted by aH . Analogously, $Ha = \{ha \mid h \in H\}$ and $aHa^{-1} = \{aha^{-1} \mid h \in H\}$. When H is a subgroup of G , the set aH is called the *left coset of H in G containing a* , whereas Ha is called the *right coset of H in G containing a* . In this case, the element a is called the *coset representative of aH (or Ha)*. We use $|aH|$ to denote the number of elements in the set aH , and $|Ha|$ to denote the number of elements in Ha .

Definition Stabilizer of a Point

Let G be a group of permutations of a set S . For each i in S , let $\text{stab}_G(i) = \{\phi \in G \mid \phi(i) = i\}$. We call $\text{stab}_G(i)$ the *stabilizer of i in G* .

Definition Orbit of a Point

Let G be a group of permutations of a set S . For each s in S , let $\text{orb}_G(s) = \{\phi(s) \mid \phi \in G\}$. The set $\text{orb}_G(s)$ is a subset of S called the *orbit of s under G* . We use $|\text{orb}_G(s)|$ to denote the number of elements in $\text{orb}_G(s)$.

Definition External Direct Product

Let $G_1, G_2, \dots, G_n$ be a finite collection of groups. The *external direct product* of $G_1, G_2, \dots, G_n$, written as $G_1 \oplus G_2 \oplus \dots \oplus G_n$, is the set of all n -tuples for which the i th component is an element of G_i and the operation is componentwise.

Definition Normal Subgroup

A subgroup H of a group G is called a *normal* subgroup of G if $aH = Ha$ for all a in G . We denote this by $H \triangleleft G$.

Definition Internal Direct Product of H and K

We say that G is the *internal direct product* of H and K and write $G = H \times K$ if H and K are normal subgroups of G and

$$G = HK \quad \text{and} \quad H \cap K = \{e\}.$$

Definition Internal Direct Product $H_1 \times H_2 \times \cdots \times H_n$

Let $H_1, H_2, \dots, H_n$ be a finite collection of normal subgroups of G . We say that G is the *internal direct product* of $H_1, H_2, \dots, H_n$ and write $G = H_1 \times H_2 \times \cdots \times H_n$, if

1. $G = H_1 H_2 \cdots H_n = \{h_1 h_2 \cdots h_n \mid h_i \in H_i\}$
2. $(H_1 H_2 \cdots H_i) \cap H_{i+1} = \{e\}$ for $i = 1, 2, \dots, n - 1$.

Definition Group Homomorphism

A *homomorphism* ϕ from a group G to a group $\bar{G}$ is a mapping from G into $\bar{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all a, b in G .

Definition Kernel of a Homomorphism

The *kernel* of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G \mid \phi(x) = e\}$. The kernel of ϕ is denoted by $\text{Ker } \phi$.

Definition Ring

A *ring* R is a set with two binary operations, addition (denoted by $a + b$) and multiplication (denoted by ab), such that for all a, b, c in R :

1. $a + b = b + a$.
2. $(a + b) + c = a + (b + c)$.
3. There is an additive identity 0 . That is, there is an element 0 in R such that $a + 0 = a$ for all a in R .
4. There is an element $-a$ in R such that $a + (-a) = 0$.
5. $a(bc) = (ab)c$.
6. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$.

Definition Subring

A subset S of a ring R is a *subring of R* if S is itself a ring with the operations of R .

Definition Zero-Divisors

A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Definition Integral Domain

An *integral domain* is a commutative ring with unity and no zero-divisors.

Definition Field

A *field* is a commutative ring with unity in which every nonzero element is a unit.

Definition Characteristic of a Ring

The *characteristic* of a ring R is the least positive integer n such that $nx = 0$ for all x in R . If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\text{char } R$.

Definition Ideal

A subring A of a ring R is called a (two-sided) *ideal* of R if for every $r \in R$ and every $a \in A$ both ra and ar are in A .

Definition Prime Ideal, Maximal Ideal

A *prime ideal* A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$. A *maximal ideal* of a commutative ring R is a *proper ideal* of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.

Definitions Ring Homomorphism, Ring Isomorphism

A *ring homomorphism* ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations; that is, for all a, b in R ,

$$\phi(a + b) = \phi(a) + \phi(b) \quad \text{and} \quad \phi(ab) = \phi(a)\phi(b).$$

A ring homomorphism that is both one-to-one and onto is called a *ring isomorphism*.

Definition Ring of Polynomials over R

Let R be a commutative ring. The set of formal symbols

$$R[x] = \{a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in R, \\ n \text{ is a nonnegative integer}\}$$

is called the *ring of polynomials over R in the indeterminate x* .

Two elements

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

and

$$b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

of $R[x]$ are considered equal if and only if $a_i = b_i$ for all nonnegative integers i . (Define $a_i = 0$ when $i > n$ and $b_i = 0$ when $i > m$.)

Definition Addition and Multiplication in $R[x]$

Let R be a commutative ring and let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

and

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

belong to $R[x]$. Then

$$f(x) + g(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + a_0 + b_0,$$

where s is the maximum of m and n , $a_i = 0$ for $i > n$, and $b_i = 0$ for $i > m$. Also,

$$f(x)g(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1x + c_0,$$

where

$$c_k = a_k b_0 + a_{k-1} b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$$

for $k = 0, \dots, m + n$.

Definition Principal Ideal Domain (PID)

A *principal ideal domain* is an integral domain R in which every ideal has the form $\langle a \rangle = \{ra \mid r \in R\}$ for some a in R .

Definition Irreducible Polynomial, Reducible Polynomial

Let D be an integral domain. A polynomial $f(x)$ from $D[x]$ that is neither the zero polynomial nor a unit in $D[x]$ is said to be *irreducible over D* if, whenever $f(x)$ is expressed as a product $f(x) = g(x)h(x)$, with $g(x)$ and $h(x)$ from $D[x]$, then $g(x)$ or $h(x)$ is a unit in $D[x]$. A nonzero, nonunit element of $D[x]$ that is not irreducible over D is called *reducible over D* .

Definition Content of Polynomial, Primitive Polynomial

The *content* of a nonzero polynomial $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$, where the a 's are integers, is the greatest common divisor of the integers $a_n, a_{n-1}, \dots, a_0$. A *primitive polynomial* is an element of $\mathbb{Z}[x]$ with content 1.

Definition Associates, Irreducibles, Primes

Elements a and b of an integral domain D are called *associates* if $a = ub$, where u is a unit of D . A nonzero element a of an integral domain D is called an *irreducible* if a is not a unit and, whenever $b, c \in D$ with $a = bc$, then b or c is a unit. A nonzero element a of an integral domain D is called a *prime* if a is not a unit and $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Definition Unique Factorization Domain (UFD)

An integral domain D is a *unique factorization domain* if

1. every nonzero element of D that is not a unit can be written as a product of irreducibles of D , and
2. the factorization into irreducibles is unique up to associates and the order in which the factors appear.

Definition Euclidean Domain

An integral domain D is called a *Euclidean domain* if there is a function d (called the *measure*) from the nonzero elements of D to the nonnegative integers such that

1. $d(a) \leq d(ab)$ for all nonzero a, b in D ; and
2. if $a, b \in D$, $b \neq 0$, then there exist elements q and r in D such that $a = bq + r$, where $r = 0$ or $d(r) < d(b)$.

Definition Vector Space

A set V is said to be a *vector space* over a field F if V is an Abelian group under addition (denoted by $+$) and, if for each $a \in F$ and $v \in V$, there is an element av in V such that the following conditions hold for all a, b in F and all u, v in V .

1. $a(v + u) = av + au$
2. $(a + b)v = av + bv$
3. $a(bv) = (ab)v$
4. $1v = v$

Definition Subspace

Let V be a vector space over a field F and let U be a subset of V . We say that U is a *subspace* of V if U is also a vector space over F under the operations of V .

Definition Linearly Dependent, Linearly Independent

A set S of vectors is said to be *linearly dependent* over the field F if there are vectors $v_1, v_2, \dots, v_n$ from S and elements $a_1, a_2, \dots, a_n$ from F , not all zero, such that $a_1v_1 + a_2v_2 + \dots + a_nv_n = 0$. A set of vectors that is not linearly dependent over F is called *linearly independent* over F .

Definition Basis

Let V be a vector space over F . A subset B of V is called a *basis* for V if B is linearly independent over F and every element of V is a linear combination of elements of B .

Definition Dimension

A vector space that has a basis consisting of n elements is said to have *dimension* n . For completeness, the trivial vector space $\{0\}$ is said to be spanned by the empty set and to have dimension 0.

Definition Extension Field

A field E is an *extension field* of a field F if $F \subseteq E$ and the operations of F are those of E restricted to F .

Definition Splitting Field

Let E be an extension field of F and let $f(x) \in F[x]$. We say that $f(x)$ *splits* in E if $f(x)$ can be factored as a product of linear factors in $E[x]$. We call E a *splitting field* for $f(x)$ over F if $f(x)$ splits in E but in no proper subfield of E .

Definition

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ belong to $F[x]$. The *derivative* of $f(x)$, denoted by $f'(x)$, is the polynomial $na_n x^{n-1} + (n-1)a_{n-1} x^{n-2} + \cdots + a_1$ in $F[x]$.

Definition

A field F is called *perfect* if F has characteristic 0 or if F has characteristic p and $F^p = \{a^p \mid a \in F\} = F$.

Definition Types of Extensions

Let E be an extension field of a field F and let $a \in E$. We call a *algebraic over* F if a is the zero of some nonzero polynomial in $F[x]$. If a is not algebraic over F , it is called *transcendental over* F . An extension E of F is called an *algebraic extension* of F if every element of E is algebraic over F . If E is not an algebraic extension of F , it is called a *transcendental extension* of F . An extension of F of the form $F(a)$ is called a *simple extension* of F .

Definition Degree of an Extension

Let E be an extension field of a field F . We say that E *has degree* n over F and write $[E:F] = n$ if E has dimension n as a vector space over F . If $[E:F]$ is finite, E is called a *finite extension* of F ; otherwise, we say that E is an *infinite extension* of F .

Definition Conjugacy Class of a

Let a and b be elements of a group G . We say that a and b are *conjugate* in G (and call b a *conjugate* of a) if $xax^{-1} = b$ for some x in G . The *conjugacy class* of a is the set $\text{cl}(a) = \{xax^{-1} \mid x \in G\}$.

Definition Sylow p -Subgroup

Let G be a finite group and let p be a prime divisor of $|G|$. If p^k divides $|G|$ and p^{k+1} does not divide $|G|$, then any subgroup of G of order p^k is called a *Sylow p -subgroup* of G .

Definition Conjugate Subgroups

Let H and K be subgroups of a group G . We say that H and K are *conjugate* in G if there is an element g in G such that $H = gKg^{-1}$.

Definition Simple Group

A group is *simple* if its only normal subgroups are the identity subgroup and the group itself.

Definition Equivalence Classes of Words

For any pair of elements u and v of $W(S)$, we say that u is related to v if v can be obtained from u by a finite sequence of insertions or deletions of words of the form xx^{-1} or $x^{-1}x$, where $x \in S$.

Definition Generators and Relations

Let G be a group generated by some subset $A = \{a_1, a_2, \dots, a_n\}$ and let F be the free group on A . Let $W = \{w_1, w_2, \dots, w_t\}$ be a subset of F and let N be the smallest normal subgroup of F containing W . We say that G is *given by the generators* $a_1, a_2, \dots, a_n$ *and the relations* $w_1 = w_2 = \dots = w_t = e$ if there is an isomorphism from F/N onto G that carries $a_i N$ to a_i .

Definition Isometry

An *isometry* of n -dimensional space $\mathbf{R}^n$ is a function from $\mathbf{R}^n$ onto $\mathbf{R}^n$ that preserves distance.

Definition Symmetry Group of a Figure in $\mathbf{R}^n$

Let F be a set of points in $\mathbf{R}^n$. The *symmetry group* of F in $\mathbf{R}^n$ is the set of all isometries of $\mathbf{R}^n$ that carry F onto itself. The group operation is function composition.

Definition Elements Fixed by ϕ

For any group G of permutations on a set S and any ϕ in G , we let $\text{fix}(\phi) = \{i \in S \mid \phi(i) = i\}$. This set is called the *elements fixed by ϕ* (or more simply, “fix of ϕ ”).

Definition Cayley Digraph of a Group

Let G be a finite group and let S be a set of generators for G . We define a digraph $\text{Cay}(S;G)$, called the *Cayley digraph of G with generating set S* , as follows.

1. Each element of G is a vertex of $\text{Cay}(S;G)$.
2. For x and y in G , there is an arc from x to y if and only if $xs = y$ for some $s \in S$.

Definition Linear Code

An (n, k) *linear code* over a finite field F is a k -dimensional subspace V of the vector space

$$F^n = \underbrace{F \oplus F \oplus \dots \oplus F}_{n \text{ copies}}$$

over F . The members of V are called the *code words*. When F is $\mathbb{Z}_2$, the code is called *binary*.

Definitions Hamming Distance, Hamming Weight

The *Hamming distance* between two vectors in F^n is the number of components in which they differ. The *Hamming weight* of a vector is the number of nonzero components of the vector. The *Hamming weight* of a linear code is the minimum weight of any nonzero vector in the code.

Definition Syndrome

If an (n, k) linear code over F has parity-check matrix H , then, for any vector u in F^n , the vector uH is called the *syndrome*[†] of u .

Definitions Automorphism, Galois Group, Fixed Field of H

Let E be an extension field of the field F . An *automorphism* of E is a ring isomorphism from E onto E . The *Galois group* of E over F , $\text{Gal}(E/F)$, is the set of all automorphisms of E that take every element of F to itself. If H is a subgroup of $\text{Gal}(E/F)$, the set

$$E_H = \{x \in E \mid \phi(x) = x \text{ for all } \phi \in H\}$$

is called the *fixed field* of H .

Definition Solvable by Radicals

Let F be a field, and let $f(x) \in F[x]$. We say that $f(x)$ is *solvable by radicals* over F if $f(x)$ splits in some extension $F(a_1, a_2, \dots, a_n)$ of F and there exist positive integers $k_1, \dots, k_n$ such that $a_1^{k_1} \in F$ and $a_i^{k_i} \in F(a_1, \dots, a_{i-1})$ for $i = 2, \dots, n$.

Definition Solvable Group

We say that a group G is *solvable* if G has a series of subgroups

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \dots \subset H_k = G,$$

where, for each $0 \leq i < k$, H_i is normal in H_{i+1} and H_{i+1}/H_i is Abelian.

Definition

For any positive integer n , let $\omega_1, \omega_2, \dots, \omega_{\phi(n)}$ denote the primitive n th roots of unity. The *n th cyclotomic polynomial* over $\mathbb{Q}$ is the polynomial $\Phi_n(x) = (x - \omega_1)(x - \omega_2) \cdots (x - \omega_{\phi(n)})$.

Theorem 0.1 Division Algorithm

Let a and b be integers with $b > 0$. Then there exist unique integers q and r with the property that $a = bq + r$, where $0 \leq r < b$.

Theorem 0.2 GCD Is a Linear Combination

For any nonzero integers a and b , there exist integers s and t such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Corollary

If a and b are relatively prime, then there exist integers s and t such that $as + bt = 1$.

Euclid's Lemma $p \mid ab$ Implies $p \mid a$ or $p \mid b$

If p is a prime that divides ab , then p divides a or p divides b .

Theorem 0.3 Fundamental Theorem of Arithmetic

Every integer greater than 1 is a prime or a product of primes. This product is unique, except for the order in which the factors appear. That is, if $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$, where the p 's and q 's are primes, then $r = s$ and, after renumbering the q 's, we have $p_i = q_i$ for all i .

Theorem 0.4 First Principle of Mathematical Induction

Let S be a set of integers containing a . Suppose S has the property that whenever some integer $n \geq a$ belongs to S , then the integer $n + 1$ also belongs to S . Then, S contains every integer greater than or equal to a .

Theorem 0.5 Second Principle of Mathematical Induction

Let S be a set of integers containing a . Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S . Then, S contains every integer greater than or equal to a .

Theorem 0.6 Equivalence Classes Partition

The equivalence classes of an equivalence relation on a set S constitute a partition of S . Conversely, for any partition P of S , there is an equivalence relation on S whose equivalence classes are the elements of P .

Theorem 0.7 Properties of Functions

Given functions $\alpha: A \rightarrow B$, $\beta: B \rightarrow C$, and $\gamma: C \rightarrow D$, then

- 1. $\gamma(\beta\alpha) = (\gamma\beta)\alpha$ (associativity).*
- 2. If α and β are one-to-one, then $\beta\alpha$ is one-to-one.*
- 3. If α and β are onto, then $\beta\alpha$ is onto.*
- 4. If α is one-to-one and onto, then there is a function α^{-1} from B onto A such that $(\alpha^{-1}\alpha)(a) = a$ for all a in A and $(\alpha\alpha^{-1})(b) = b$ for all b in B .*

Theorem 2.1 Uniqueness of the Identity

In a group G , there is only one identity element.

Theorem 2.2 Cancellation

In a group G , the right and left cancellation laws hold; that is, $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.

Theorem 2.3 Uniqueness of Inverses

For each element a in a group G , there is a unique element b in G such that $ab = ba = e$.

Theorem 2.4 Socks-Shoes Property

For group elements a and b , $(ab)^{-1} = b^{-1}a^{-1}$.

Theorem 3.1 One-Step Subgroup Test

Let G be a group and H a nonempty subset of G . If ab^{-1} is in H whenever a and b are in H , then H is a subgroup of G . (In additive notation, if $a - b$ is in H whenever a and b are in H , then H is a subgroup of G .)

Theorem 3.2 Two-Step Subgroup Test

Let G be a group and let H be a nonempty subset of G . If ab is in H whenever a and b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G .

Theorem 3.3 Finite Subgroup Test

Let H be a nonempty finite subset of a group G . If H is closed under the operation of G , then H is a subgroup of G .

Theorem 3.4 $\langle a \rangle$ Is a Subgroup

Let G be a group, and let a be any element of G . Then, $\langle a \rangle$ is a subgroup of G .

Theorem 3.5 Center Is a Subgroup

The center of a group G is a subgroup of G .

Theorem 3.6 $C(a)$ Is a Subgroup

For each a in a group G , the centralizer of a is a subgroup of G .

Theorem 4.1 Criterion for $a^i = a^j$

Let G be a group, and let a belong to G . If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order, say, n , then $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i - j$.

Corollary 1 $|a| = |\langle a \rangle|$

For any group element a , $|a| = |\langle a \rangle|$.

Corollary 2 $a^k = e$ Implies That $|a|$ Divides k

Let G be a group and let a be an element of order n in G . If $a^k = e$, then n divides k .

Theorem 4.2 $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$

Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ and $|a^k| = n/\gcd(n,k)$.

Corollary 1 Orders of Elements in Finite Cyclic Groups

In a finite cyclic group, the order of an element divides the order of the group.

Corollary 2 Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$

Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\gcd(n, i) = \gcd(n, j)$ and $|a^i| = |a^j|$ if and only if $\gcd(n, i) = \gcd(n, j)$.

Corollary 3 Generators of Finite Cyclic Groups

Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $\gcd(n, j) = 1$ and $|a| = |\langle a^j \rangle|$ if and only if $\gcd(n, j) = 1$.

Corollary 4 Generators of Z_n

An integer k in Z_n is a generator of Z_n if and only if $\gcd(n, k) = 1$.

Theorem 4.3 Fundamental Theorem of Cyclic Groups

Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n ; and, for each positive divisor k of n , the group $\langle a \rangle$ has exactly one subgroup of order k —namely, $\langle a^{n/k} \rangle$.

Corollary Subgroups of Z_n

For each positive divisor k of n , the set $\langle n/k \rangle$ is the unique subgroup of Z_n of order k ; moreover, these are the only subgroups of Z_n .

Theorem 4.4 Number of Elements of Each Order in a Cyclic Group

If d is a positive divisor of n , the number of elements of order d in a cyclic group of order n is $\phi(d)$.

Corollary Number of Elements of Order d in a Finite Group

In a finite group, the number of elements of order d is divisible by $\phi(d)$.

Theorem 5.1 Products of Disjoint Cycles

Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.

Theorem 5.2 Disjoint Cycles Commute

If the pair of cycles $\alpha = (a_1, a_2, \dots, a_m)$ and $\beta = (b_1, b_2, \dots, b_n)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

Theorem 5.3 Order of a Permutation (Ruffini—1799)

The order of a permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.

Theorem 5.4 Product of 2-Cycles

Every permutation in S_n , $n > 1$, is a product of 2-cycles.

Lemma

If $\varepsilon = \beta_1\beta_2 \cdots \beta_r$, where the β 's are 2-cycles, then r is even.

Theorem 5.5 Always Even or Always Odd

If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even (odd) number of 2-cycles. In symbols, if

$$\alpha = \beta_1\beta_2 \cdots \beta_r \quad \text{and} \quad \alpha = \gamma_1\gamma_2 \cdots \gamma_s,$$

where the β 's and the γ 's are 2-cycles, then r and s are both even or both odd.

Theorem 5.6 Even Permutations Form a Group

The set of even permutations in S_n forms a subgroup of S_n .

Theorem 5.7

For $n > 1$, A_n has order $n!/2$.

Theorem 6.1 Cayley's Theorem (1854)

Every group is isomorphic to a group of permutations.

Theorem 6.2 Properties of Isomorphisms Acting on Elements

Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. ϕ carries the identity of G to the identity of $\overline{G}$.
2. For every integer n and for every group element a in G , $\phi(a^n) = [\phi(a)]^n$.
3. For any elements a and b in G , a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.
4. $G = \langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$.
5. $|a| = |\phi(a)|$ for all a in G (isomorphisms preserve orders).
6. For a fixed integer k and a fixed group element b in G , the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\overline{G}$.
7. If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

Theorem 6.3 Properties of Isomorphisms Acting on Groups

Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then

1. ϕ^{-1} is an isomorphism from $\overline{G}$ onto G .
2. G is Abelian if and only if $\overline{G}$ is Abelian.
3. G is cyclic if and only if $\overline{G}$ is cyclic.
4. If K is a subgroup of G , then $\phi(K) = \{\phi(k) \mid k \in K\}$ is a subgroup of $\overline{G}$.

Theorem 6.4 $\text{Aut}(G)$ and $\text{Inn}(G)$ Are Groups[†]

The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.

Theorem 6.5 $\text{Aut}(Z_n) \approx U(n)$

For every positive integer n , $\text{Aut}(Z_n)$ is isomorphic to $U(n)$.

Lemma Properties of Cosets

Let H be a subgroup of G , and let a and b belong to G . Then,

1. $a \in aH$,
2. $aH = H$ if and only if $a \in H$,
3. $aH = bH$ if and only if $a \in bH$
4. $aH = bH$ or $aH \cap bH = \emptyset$,
5. $aH = bH$ if and only if $a^{-1}b \in H$,
6. $|aH| = |bH|$,
7. $aH = Ha$ if and only if $H = aHa^{-1}$,
8. aH is a subgroup of G if and only if $a \in H$.

Theorem 7.1 Lagrange's Theorem[†]: $|H|$ Divides $|G|$

If G is a finite group and H is a subgroup of G , then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$.

Corollary 1 $|G:H| = |G|/|H|$

If G is a finite group and H is a subgroup of G , then $|G:H| = |G|/|H|$.

Corollary 2 $|a|$ Divides $|G|$

In a finite group, the order of each element of the group divides the order of the group.

Corollary 3 Groups of Prime Order Are Cyclic

A group of prime order is cyclic.

Corollary 4 $a^{|G|} = e$

Let G be a finite group, and let $a \in G$. Then, $a^{|G|} = e$.

Corollary 5 Fermat's Little Theorem

For every integer a and every prime p , $a^p \bmod p = a \bmod p$.

Theorem 7.2 Classification of Groups of Order $2p$

Let G be a group of order $2p$, where p is a prime greater than 2. Then G is isomorphic to Z_{2p} or D_p .

Theorem 7.3 Orbit-Stabilizer Theorem

Let G be a finite group of permutations of a set S . Then, for any i from S , $|G| = |\text{orb}_G(i)| |\text{stab}_G(i)|$.

Theorem 7.4 The Rotation Group of a Cube

The group of rotations of a cube is isomorphic to S_4 .

Theorem 8.1 Order of an Element in a Direct Product

The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,

$$|(g_1, g_2, \dots, g_n)| = \text{lcm}(|g_1|, |g_2|, \dots, |g_n|).$$

Theorem 8.2 Criterion for $G \oplus H$ to be Cyclic

Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

Corollary 1 Criterion for $G_1 \oplus G_2 \oplus \dots \oplus G_n$ to Be Cyclic

An external direct product $G_1 \oplus G_2 \oplus \dots \oplus G_n$ of a finite number of finite cyclic groups is cyclic if and only if $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$.

Corollary 2 Criterion for $Z_{n_1 n_2 \dots n_k} \approx Z_{n_1} \oplus Z_{n_2} \oplus \dots \oplus Z_{n_k}$

Let $m = n_1 n_2 \dots n_k$. Then Z_m is isomorphic to $Z_{n_1} \oplus Z_{n_2} \oplus \dots \oplus Z_{n_k}$ if and only if n_i and n_j are relatively prime when $i \neq j$.

Theorem 8.3 $U(n)$ as an External Direct Product

Suppose s and t are relatively prime. Then $U(st)$ is isomorphic to the external direct product of $U(s)$ and $U(t)$. In short,

$$U(st) \approx U(s) \oplus U(t).$$

Moreover, $U_s(st)$ is isomorphic to $U(t)$ and $U_t(st)$ is isomorphic to $U(s)$.

Corollary

Let $m = n_1 n_2 \cdots n_k$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then,

$$U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k).$$

Theorem 9.1 Normal Subgroup Test

A subgroup H of G is normal in G if and only if $xHx^{-1} \subseteq H$ for all x in G .

Theorem 9.2 Factor Groups (O. Hölder, 1889)

Let G be a group and let H be a normal subgroup of G . The set $G/H = \{aH \mid a \in G\}$ is a group under the operation $(aH)(bH) = abH$.[†]

Theorem 9.3 The G/Z Theorem

Let G be a group and let $Z(G)$ be the center of G . If $G/Z(G)$ is cyclic, then G is Abelian.

Theorem 9.4 $G/Z(G) \approx \text{Inn}(G)$

For any group G , $G/Z(G)$ is isomorphic to $\text{Inn}(G)$.

Theorem 9.5 Cauchy's Theorem for Abelian Groups

Let G be a finite Abelian group and let p be a prime that divides the order of G . Then G has an element of order p .

Theorem 9.6 $H_1 \times H_2 \times \cdots \times H_n \approx H_1 \oplus H_2 \oplus \cdots \oplus H_n$

If a group G is the internal direct product of a finite number of subgroups $H_1, H_2, \dots, H_n$, then G is isomorphic to the external direct product of $H_1, H_2, \dots, H_n$.

Theorem 9.7 Classification of Groups of Order p^2

Every group of order p^2 , where p is a prime, is isomorphic to Z_{p^2} or $Z_p \oplus Z_p$.

Corollary

If G is a group of order p^2 , where p is a prime, then G is Abelian.

Theorem 10.1 Properties of Elements Under Homomorphisms

Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let g be an element of G . Then

1. ϕ carries the identity of G to the identity of $\overline{G}$.
2. $\phi(g^n) = (\phi(g))^n$ for all n in $\mathbb{Z}$.
3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.
4. $\text{Ker } \phi$ is a subgroup of G .
5. $\phi(a) = \phi(b)$ if and only if $a\text{Ker } \phi = b\text{Ker } \phi$.
6. If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\text{Ker } \phi$.

Theorem 10.2 Properties of Subgroups Under Homomorphisms

Let ϕ be a homomorphism from a group G to a group $\bar{G}$ and let H be a subgroup of G . Then

1. $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\bar{G}$.
2. If H is cyclic, then $\phi(H)$ is cyclic.
3. If H is Abelian, then $\phi(H)$ is Abelian.
4. If H is normal in G , then $\phi(H)$ is normal in $\phi(G)$.
5. If $|\text{Ker } \phi| = n$, then ϕ is an n -to-1 mapping from G onto $\phi(G)$.
6. If $|H| = n$, then $|\phi(H)|$ divides n .
7. If $\bar{K}$ is a subgroup of $\bar{G}$, then $\phi^{-1}(\bar{K}) = \{k \in G \mid \phi(k) \in \bar{K}\}$ is a subgroup of G .
8. If $\bar{K}$ is a normal subgroup of $\bar{G}$, then $\phi^{-1}(\bar{K}) = \{k \in G \mid \phi(k) \in \bar{K}\}$ is a normal subgroup of G .
9. If ϕ is onto and $\text{Ker } \phi = \{e\}$, then ϕ is an isomorphism from G to $\bar{G}$.

Corollary Kernels Are Normal

Let ϕ be a group homomorphism from G to $\bar{G}$. Then $\text{Ker } \phi$ is a normal subgroup of G .

Theorem 10.3 First Isomorphism Theorem (Jordan, 1870)

Let ϕ be a group homomorphism from G to $\bar{G}$. Then the mapping from $G/\text{Ker } \phi$ to $\phi(G)$, given by $g\text{Ker } \phi \rightarrow \phi(g)$, is an isomorphism. In symbols, $G/\text{Ker } \phi \approx \phi(G)$.

Theorem 10.4 Normal Subgroups Are Kernels

Corollary

Every normal subgroup of a group G is the kernel of a homomorphism of G . In particular, a normal subgroup N is the kernel of the mapping $g \rightarrow gN$ from G to G/N .

If ϕ is a homomorphism from a finite group G to $\bar{G}$, then $|\phi(G)|$ divides $|G|$ and $|\bar{G}|$.

Theorem 10.4 Normal Subgroups Are Kernels

Every normal subgroup of a group G is the kernel of a homomorphism of G . In particular, a normal subgroup N is the kernel of the mapping $g \rightarrow gN$ from G to G/N .

Theorem 11.1 Fundamental Theorem of Finite Abelian Groups

Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

Corollary Existence of Subgroups of Abelian Groups

If m divides the order of a finite Abelian group G , then G has a subgroup of order m .

Lemma 1

Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m . Then $G = H \times K$, where $H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$. Moreover, $|H| = p^n$.

Lemma 2

Let G be an Abelian group of prime-power order and let a be an element of maximal order in G . Then G can be written in the form $\langle a \rangle \times K$.

Lemma 3

A finite Abelian group of prime-power order is an internal direct product of cyclic groups.

Lemma 4

Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times H_2 \times \cdots \times H_m$ and $G = K_1 \times K_2 \times \cdots \times K_n$, where the H 's and K 's are nontrivial cyclic subgroups with $|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ and $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i .

Theorem 12.1 Rules of Multiplication

Let a , b , and c belong to a ring R . Then

1. $a0 = 0a = 0$.
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$.[†]
4. $a(b - c) = ab - ac$ and $(b - c)a = ba - ca$.

Furthermore, if R has a unity element 1 , then

5. $(-1)a = -a$.
6. $(-1)(-1) = 1$.

Theorem 12.2 Uniqueness of the Unity and Inverses

If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.

Theorem 12.3 Subring Test

A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication—that is, if $a - b$ and ab are in S whenever a and b are in S .

Theorem 13.1 Cancellation

Let a , b , and c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.

Theorem 13.2 Finite Integral Domains Are Fields

A finite integral domain is a field.

Corollary $\mathbb{Z}_p$ Is a Field

For every prime p , $\mathbb{Z}_p$, the ring of integers modulo p , is a field.

Theorem 13.3 Characteristic of a Ring with Unity

Let R be a ring with unity 1 . If 1 has infinite order under addition, then the characteristic of R is 0 . If 1 has order n under addition, then the characteristic of R is n .

Theorem 13.4 Characteristic of an Integral Domain

The characteristic of an integral domain is 0 or prime.

Theorem 14.1 Ideal Test

A nonempty subset A of a ring R is an ideal of R if

- $a - b \in A$ whenever $a, b \in A$.*
- ra and ar are in A whenever $a \in A$ and $r \in R$.*

Theorem 14.2 Existence of Factor Rings

Let R be a ring and let A be a subring of R . The set of cosets $\{r + A \mid r \in R\}$ is a ring under the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R .

Theorem 14.3 R/A Is an Integral Domain If and Only If A Is Prime

Let R be a commutative ring with unity and let A be an ideal of R . Then R/A is an integral domain if and only if A is prime.

Theorem 14.4 R/A Is a Field If and Only If A Is Maximal

Let R be a commutative ring with unity and let A be an ideal of R . Then R/A is a field if and only if A is maximal.

Theorem 15.1 Properties of Ring Homomorphisms

Let ϕ be a ring homomorphism from a ring R to a ring S . Let A be a subring of R and let B be an ideal of S .

1. For any $r \in R$ and any positive integer n , $\phi(nr) = n\phi(r)$ and $\phi(r^n) = (\phi(r))^n$.
2. $\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of S .
3. If A is an ideal and ϕ is onto S , then $\phi(A)$ is an ideal.
4. $\phi^{-1}(B) = \{r \in R \mid \phi(r) \in B\}$ is an ideal of R .
5. If R is commutative, then $\phi(R)$ is commutative.
6. If R has a unity 1 , $S \neq \{0\}$, and ϕ is onto, then $\phi(1)$ is the unity of S .
7. ϕ is an isomorphism if and only if ϕ is onto and $\text{Ker } \phi = \{r \in R \mid \phi(r) = 0\} = \{0\}$.
8. If ϕ is an isomorphism from R onto S , then ϕ^{-1} is an isomorphism from S onto R .

Theorem 15.2 Kernels Are Ideals

Let ϕ be a ring homomorphism from a ring R to a ring S . Then $\text{Ker } \phi = \{r \in R \mid \phi(r) = 0\}$ is an ideal of R .

Theorem 15.3 First Isomorphism Theorem for Rings

Let ϕ be a ring homomorphism from R to S . Then the mapping from $R/\text{Ker } \phi$ to $\phi(R)$, given by $r + \text{Ker } \phi \rightarrow \phi(r)$, is an isomorphism. In symbols, $R/\text{Ker } \phi \approx \phi(R)$.

Theorem 15.4 Ideals Are Kernels

Every ideal of a ring R is the kernel of a ring homomorphism of R . In particular, an ideal A is the kernel of the mapping $r \rightarrow r + A$ from R to R/A .

Theorem 15.5 Homomorphism from $\mathbb{Z}$ to a Ring with Unity

Let R be a ring with unity 1 . The mapping $\phi: \mathbb{Z} \rightarrow R$ given by $n \rightarrow n \cdot 1$ is a ring homomorphism.

Corollary 1 A Ring with Unity Contains $\mathbb{Z}_n$ or $\mathbb{Z}$

If R is a ring with unity and the characteristic of R is $n > 0$, then R contains a subring isomorphic to $\mathbb{Z}_n$. If the characteristic of R is 0 , then R contains a subring isomorphic to $\mathbb{Z}$.

Corollary 2 $\mathbb{Z}_m$ Is a Homomorphic Image of $\mathbb{Z}$

For any positive integer m , the mapping of $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_m$ given by $x \rightarrow x \bmod m$ is a ring homomorphism.

Corollary 3 A Field Contains $\mathbb{Z}_p$ or $\mathbb{Q}$ (Steinitz, 1910)

If F is a field of characteristic p , then F contains a subfield isomorphic to $\mathbb{Z}_p$. If F is a field of characteristic 0, then F contains a subfield isomorphic to the rational numbers.

Theorem 15.6 Field of Quotients

Let D be an integral domain. Then there exists a field F (called the field of quotients of D) that contains a subring isomorphic to D .

Theorem 16.1 D an Integral Domain Implies $D[x]$ an Integral Domain

If D is an integral domain, then $D[x]$ is an integral domain.

Theorem 16.2 Division Algorithm for $F[x]$

Let F be a field and let $f(x)$ and $g(x) \in F[x]$ with $g(x) \neq 0$. Then there exist unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

Corollary 1 The Remainder Theorem

Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then $f(a)$ is the remainder in the division of $f(x)$ by $x - a$.

Corollary 2 The Factor Theorem

Let F be a field, $a \in F$, and $f(x) \in F[x]$. Then a is a zero of $f(x)$ if and only if $x - a$ is a factor of $f(x)$.

Corollary 3 Polynomials of Degree n Have at Most n Zeros

A polynomial of degree n over a field has at most n zeros, counting multiplicity.

Theorem 16.3 $F[x]$ Is a PID

Let F be a field. Then $F[x]$ is a principal ideal domain.

Theorem 16.4 Criterion for $I = \langle g(x) \rangle$

Let F be a field, I a nonzero ideal in $F[x]$, and $g(x)$ an element of $F[x]$. Then, $I = \langle g(x) \rangle$ if and only if $g(x)$ is a nonzero polynomial of minimum degree in I .

Theorem 17.1 Reducibility Test for Degrees 2 and 3

Let F be a field. If $f(x) \in F[x]$ and $\deg f(x)$ is 2 or 3, then $f(x)$ is reducible over F if and only if $f(x)$ has a zero in F .

Gauss's Lemma

The product of two primitive polynomials is primitive.

Theorem 17.2 Reducibility over $\mathbb{Q}$ Implies Reducibility Over $\mathbb{Z}$

Let $f(x) \in \mathbb{Z}[x]$. If $f(x)$ is reducible over $\mathbb{Q}$, then it is reducible over $\mathbb{Z}$.

Theorem 17.3 Mod p Irreducibility Test

Let p be a prime and suppose that $f(x) \in \mathbb{Z}[x]$ with $\deg f(x) \geq 1$. Let $\bar{f}(x)$ be the polynomial in $\mathbb{Z}_p[x]$ obtained from $f(x)$ by reducing all the coefficients of $f(x)$ modulo p . If $\bar{f}(x)$ is irreducible over $\mathbb{Z}_p$ and $\deg \bar{f}(x) = \deg f(x)$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Theorem 17.4 Eisenstein's Criterion (1850)

Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x].$$

If there is a prime p such that $p \nmid a_n$, $p \mid a_{n-1}, \dots, p \mid a_0$ and $p^2 \nmid a_0$, then $f(x)$ is irreducible over $\mathbb{Q}$.

Corollary Irreducibility of p th Cyclotomic Polynomial

For any prime p , the p th cyclotomic polynomial

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

is irreducible over $\mathbb{Q}$.

Theorem 17.5 $\langle p(x) \rangle$ Is Maximal If and Only If $p(x)$ Is Irreducible

Let F be a field and let $p(x) \in F[x]$. Then $\langle p(x) \rangle$ is a maximal ideal in $F[x]$ if and only if $p(x)$ is irreducible over F .

Corollary 1 $F[x]/\langle p(x) \rangle$ Is a Field

Let F be a field and $p(x)$ an irreducible polynomial over F . Then $F[x]/\langle p(x) \rangle$ is a field.

Corollary 2 $p(x) \mid a(x)b(x)$ Implies $p(x) \mid a(x)$ or $p(x) \mid b(x)$

Let F be a field and let $p(x), a(x), b(x) \in F[x]$. If $p(x)$ is irreducible over F and $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

Theorem 17.6 Unique Factorization in $\mathbb{Z}[x]$

Every polynomial in $\mathbb{Z}[x]$ that is not the zero polynomial or a unit in $\mathbb{Z}[x]$ can be written in the form $b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x)$, where the b_i 's are irreducible polynomials of degree 0, and the $p_i(x)$'s are irreducible polynomials of positive degree. Furthermore, if

$$b_1 b_2 \cdots b_s p_1(x) p_2(x) \cdots p_m(x) = c_1 c_2 \cdots c_t q_1(x) q_2(x) \cdots q_n(x),$$

where the b 's and c 's are irreducible polynomials of degree 0, and the $p(x)$'s and $q(x)$'s are irreducible polynomials of positive degree, then $s = t$, $m = n$, and, after renumbering the c 's and $q(x)$'s, we have $b_i = \pm c_i$ for $i = 1, \dots, s$; and $p_i(x) = \pm q_i(x)$ for $i = 1, \dots, m$.

Theorem 18.1 Prime Implies Irreducible

In an integral domain, every prime is an irreducible.

Theorem 18.2 PID Implies Irreducible Equals Prime

In a principal ideal domain, an element is an irreducible if and only if it is a prime.

Lemma Ascending Chain Condition for a PID

In a principal ideal domain, any strictly increasing chain of ideals $I_1 \subset I_2 \subset \cdots$ must be finite in length.

Theorem 18.3 PID Implies UFD

Every principal ideal domain is a unique factorization domain.

Corollary $F[x]$ is a UFD

Let F be a field. Then $F[x]$ is a unique factorization domain.

Theorem 18.4 ED (Euclidean Domain) Implies PID

Every Euclidean domain is a principal ideal domain.

Corollary ED Implies UFD

Every Euclidean domain is a unique factorization domain.

Theorem 18.5 D a UFD Implies $D[x]$ a UFD

If D is a unique factorization domain, then $D[x]$ is a unique factorization domain.

Theorem 19.1 Invariance of Basis Size

If $\{u_1, u_2, \dots, u_m\}$ and $\{w_1, w_2, \dots, w_n\}$ are both bases of a vector space V over a field F , then $m = n$.

Theorem 20.1 Fundamental Theorem of Field Theory (Kronecker's Theorem, 1887)

Let F be a field and let $f(x)$ be a nonconstant polynomial in $F[x]$. Then there is an extension field E of F in which $f(x)$ has a zero.

Theorem 20.2 Existence of Splitting Fields

Let F be a field and let $f(x)$ be a nonconstant element of $F[x]$. Then there exists a splitting field E for $f(x)$ over F .

Theorem 20.3 $F(a) \approx F[x]/\langle p(x) \rangle$

Let F be a field and let $p(x) \in F[x]$ be irreducible over F . If a is a zero of $p(x)$ in some extension E of F , then $F(a)$ is isomorphic to $F[x]/\langle p(x) \rangle$. Furthermore, if $\deg p(x) = n$, then every member of $F(a)$ can be uniquely expressed in the form

$$c_{n-1}a^{n-1} + c_{n-2}a^{n-2} + \dots + c_1a + c_0,$$

where $c_0, c_1, \dots, c_{n-1} \in F$.

Corollary $F(a) \approx F(b)$

Let F be a field and let $p(x) \in F[x]$ be irreducible over F . If a is a zero of $p(x)$ in some extension E of F and b is a zero of $p(x)$ in some extension E' of F , then the fields $F(a)$ and $F(b)$ are isomorphic.

Lemma

Let F be a field, let $p(x) \in F[x]$ be irreducible over F , and let a be a zero of $p(x)$ in some extension of F . If ϕ is a field isomorphism from F to F' and b is a zero of $\phi(p(x))$ in some extension of F' , then there is an isomorphism from $F(a)$ to $F'(b)$ that agrees with ϕ on F and carries a to b .

Theorem 20.4 Extending $\phi: F \rightarrow F'$

Let ϕ be an isomorphism from a field F to a field F' and let $f(x) \in F[x]$. If E is a splitting field for $f(x)$ over F and E' is a splitting field for $\phi(f(x))$ over F' , then there is an isomorphism from E to E' that agrees with ϕ on F .

Corollary Splitting Fields Are Unique

Let F be a field and let $f(x) \in F[x]$. Then any two splitting fields of $f(x)$ over F are isomorphic.

Lemma Properties of the Derivative

Let $f(x)$ and $g(x) \in F[x]$ and let $a \in F$. Then

1. $(f(x) + g(x))' = f'(x) + g'(x)$
2. $(af(x))' = af'(x)$
3. $(f(x)g(x))' = f(x)g'(x) + g(x)f'(x)$.

Theorem 20.5 Criterion for Multiple Zeros

A polynomial $f(x)$ over a field F has a multiple zero in some extension E if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree in $F[x]$.

Theorem 20.6 Zeros of an Irreducible

Let $f(x)$ be an irreducible polynomial over a field F . If F has characteristic 0, then $f(x)$ has no multiple zeros. If F has characteristic $p \neq 0$, then $f(x)$ has a multiple zero only if it is of the form $f(x) = g(x^p)$ for some $g(x)$ in $F[x]$.

Theorem 20.7 Finite Fields Are Perfect

Every finite field is perfect.

Theorem 20.8 Criterion for No Multiple Zeros

If $f(x)$ is an irreducible polynomial over a perfect field F , then $f(x)$ has no multiple zeros.

Theorem 20.9 Zeros of an Irreducible over a Splitting Field

Let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$ over F . Then all the zeros of $f(x)$ in E have the same multiplicity.

Corollary Factorization of an Irreducible over a Splitting Field

Let $f(x)$ be an irreducible polynomial over a field F and let E be a splitting field of $f(x)$. Then $f(x)$ has the form

$$a(x - a_1)^n(x - a_2)^n \cdots (x - a_r)^n$$

where $a_1, a_2, \dots, a_r$ are distinct elements of E and $a \in F$.

Theorem 21.1 Characterization of Extensions

Let E be an extension field of the field F and let $a \in E$. If a is transcendental over F , then $F(a) \approx F(x)$. If a is algebraic over F , then $F(a) \approx F[x]/\langle p(x) \rangle$, where $p(x)$ is a polynomial in $F[x]$ of minimum degree such that $p(a) = 0$. Moreover, $p(x)$ is irreducible over F .

Theorem 21.2 Uniqueness Property

If a is algebraic over a field F , then there is a unique monic irreducible polynomial $p(x)$ in $F[x]$ such that $p(a) = 0$.

Theorem 21.3 Divisibility Property

Let a be algebraic over F , and let $p(x)$ be the minimal polynomial for a over F . If $f(x) \in F[x]$ and $f(a) = 0$, then $p(x)$ divides $f(x)$ in $F[x]$.

Theorem 21.4 Finite Implies Algebraic

If E is a finite extension of F , then E is an algebraic extension of F .

Theorem 21.5 $[K:F] = [K:E][E:F]$

Let K be a finite extension field of the field E and let E be a finite extension field of the field F . Then K is a finite extension field of F and $[K:F] = [K:E][E:F]$.

Theorem 21.6 Primitive Element Theorem (Steinitz, 1910)

If F is a field of characteristic 0, and a and b are algebraic over F , then there is an element c in $F(a, b)$ such that $F(a, b) = F(c)$.

Theorem 21.7 Algebraic over Algebraic Is Algebraic

If K is an algebraic extension of E and E is an algebraic extension of F , then K is an algebraic extension of F .

Corollary Subfield of Algebraic Elements

Let E be an extension field of the field F . Then the set of all elements of E that are algebraic over F is a subfield of E .

Theorem 22.1 Classification of Finite Fields

For each prime p and each positive integer n , there is, up to isomorphism, a unique finite field of order p^n .

Theorem 22.2 Structure of Finite Fields

As a group under addition, $\text{GF}(p^n)$ is isomorphic to

$$\underbrace{Z_p \oplus Z_p \oplus \cdots \oplus Z_p}_{n \text{ factors}}$$

As a group under multiplication, the set of nonzero elements of $\text{GF}(p^n)$ is isomorphic to Z_{p^n-1} (and is, therefore, cyclic).

Corollary 1

$$[\text{GF}(p^n):\text{GF}(p)] = n$$

Corollary 2 $\text{GF}(p^n)$ Contains an Element of Degree n

Let a be a generator of the group of nonzero elements of $\text{GF}(p^n)$ under multiplication. Then a is algebraic over $\text{GF}(p)$ of degree n .

Theorem 22.3 Subfields of a Finite Field

For each divisor m of n , $\text{GF}(p^n)$ has a unique subfield of order p^m . Moreover, these are the only subfields of $\text{GF}(p^n)$.

Theorem 24.1 The Number of Conjugates of a

Let G be a finite group and let a be an element of G . Then, $|\text{cl}(a)| = |G:C(a)|$.

Corollary 1 $|\text{cl}(a)|$ Divides $|G|$

In a finite group, $|\text{cl}(a)|$ divides $|G|$.

Corollary 2 The Class Equation

For any finite group G ,

$$|G| = \sum |G:C(a)|,$$

where the sum runs over one element a from each conjugacy class of G .

Theorem 24.2 p -Groups Have Nontrivial Centers

Let G be a nontrivial finite group whose order is a power of a prime p . Then $Z(G)$ has more than one element.

Corollary Groups of Order p^2 Are Abelian

If $|G| = p^2$, where p is prime, then G is Abelian.

Theorem 24.3 Existence of Subgroups of Prime-Power Order (Sylow's First Theorem, 1872)

Let G be a finite group and let p be a prime. If p^k divides $|G|$, then G has at least one subgroup of order p^k .

Corollary Cauchy's Theorem

Let G be a finite group and let p be a prime that divides the order of G . Then G has an element of order p .

Theorem 24.4 Sylow's Second Theorem

If H is a subgroup of a finite group G and $|H|$ is a power of a prime p , then H is contained in some Sylow p -subgroup of G .

Theorem 24.5 Sylow's Third Theorem

Let p be a prime and let G be a group of order $p^k m$, where p does not divide m . Then the number n of Sylow p -subgroups of G is equal to 1 modulo p and divides m . Furthermore, any two Sylow p -subgroups of G are conjugate.

Corollary A Unique Sylow p -Subgroup Is Normal

A Sylow p -subgroup of a finite group G is a normal subgroup of G if and only if it is the only Sylow p -subgroup of G .

Theorem 24.6 Cyclic Groups of Order pq

If G is a group of order pq , where p and q are primes, $p < q$, and p does not divide $q - 1$, then G is cyclic. In particular, G is isomorphic to Z_{pq} .

Theorem 25.1 Sylow Test for Nonsimplicity

Let n be a positive integer that is not prime, and let p be a prime divisor of n . If 1 is the only divisor of n that is equal to 1 modulo p , then there does not exist a simple group of order n .

Theorem 25.2 2 · Odd Test

An integer of the form $2 \cdot n$, where n is an odd number greater than 1, is not the order of a simple group.

Theorem 25.3 Generalized Cayley Theorem

Let G be a group and let H be a subgroup of G . Let S be the group of all permutations of the left cosets of H in G . Then there is a homomorphism from G into S whose kernel lies in H and contains every normal subgroup of G that is contained in H .

Corollary 1 Index Theorem

If G is a finite group and H is a proper subgroup of G such that $|G|$ does not divide $|G:H|!$, then H contains a nontrivial normal subgroup of G . In particular, G is not simple.

Corollary 2 Embedding Theorem

If a finite non-Abelian simple group G has a subgroup of index n , then G is isomorphic to a subgroup of A_n .

Theorem 26.1 Equivalence Classes Form a Group

Let S be a set of distinct symbols. For any word u in $W(S)$, let $\bar{u}$ denote the set of all words in $W(S)$ equivalent to u (that is, $\bar{u}$ is the equivalence class containing u). Then the set of all equivalence classes of elements of $W(S)$ is a group under the operation $\bar{u} \cdot \bar{v} = \overline{uv}$.

Theorem 26.2 The Universal Mapping Property

Every group is a homomorphic image of a free group.

Corollary Universal Factor Group Property

Every group is isomorphic to a factor group of a free group.

Theorem 26.3 (Dyck, 1882)

Let

$$G = \langle a_1, a_2, \dots, a_n \mid w_1 = w_2 = \dots = w_t = e \rangle$$

and let

$$\bar{G} = \langle a_1, a_2, \dots, a_n \mid w_1 = w_2 = \dots = w_t = w_{t+1} = \dots = w_{t+k} = e \rangle.$$

Then $\bar{G}$ is a homomorphic image of G .

Corollary Largest Group Satisfying Defining Relations

If K is a group satisfying the defining relations of a finite group G and $|K| \geq |G|$, then K is isomorphic to G .

Theorem 26.4 Classification of Groups of Order 8 (Cayley, 1859)

Up to isomorphism, there are only five groups of order 8: Z_8 , $Z_4 \oplus Z_2$, $Z_2 \oplus Z_2 \oplus Z_2$, D_4 , and the quaternions.

Theorem 26.5 Characterization of Dihedral Groups

Any group generated by a pair of elements of order 2 is dihedral.

Theorem 27.1 Finite Symmetry Groups in the Plane

The only finite plane symmetry groups are Z_n and D_n .

Theorem 27.2 Finite Groups of Rotations in $\mathbb{R}^3$

Up to isomorphism, the finite groups of rotations in $\mathbb{R}^3$ are Z_n , D_n , A_4 , S_4 , and A_5 .

Theorem 29.1 (Burnside)

If G is a finite group of permutations on a set S , then the number of orbits of elements of S under G is

$$\frac{1}{|G|} \sum_{\phi \in G} |\text{fix}(\phi)|.$$

Theorem 30.1 A Necessary Condition

$\text{Cay}(\{(1, 0), (0, 1)\}; Z_m \oplus Z_n)$ does not have a Hamiltonian circuit when m and n are relatively prime and greater than 1.

Theorem 30.2 A Sufficient Condition

$\text{Cay}(\{(1, 0), (0, 1)\}; Z_m \oplus Z_n)$ has a Hamiltonian circuit when n divides m .

Theorem 30.3 Abelian Groups Have Hamiltonian Paths

Let G be a finite Abelian group, and let S be any (nonempty[†]) generating set for G . Then $\text{Cay}(S; G)$ has a Hamiltonian path.

Theorem 31.1 Properties of Hamming Distance and Hamming Weight

For any vectors u , v , and w , $d(u, v) \leq d(u, w) + d(w, v)$ and $d(u, v) = \text{wt}(u - v)$.

Theorem 31.2 Correcting Capability of a Linear Code

If the Hamming weight of a linear code is at least $2t + 1$, then the code can correct any t or fewer errors. Alternatively, the same code can detect any $2t$ or fewer errors.

Lemma Orthogonality Relation

Let C be a systematic (n, k) linear code over F with a standard generator matrix G and parity-check matrix H . Then, for any vector v in F^n , we have $vH = 0$ (the zero vector) if and only if v belongs to C .

Theorem 31.3 Parity-Check Matrix Decoding

Parity-check matrix decoding will correct any single error if and only if the rows of the parity-check matrix are nonzero and no one row is a scalar multiple of any other row.

Theorem 31.4 Coset Decoding Is Nearest-Neighbor Decoding

In coset decoding, a received word w is decoded as a code word c such that $d(w, c)$ is a minimum.

Theorem 31.5 Same Coset—Same Syndrome

Let C be an (n, k) linear code over F with a parity-check matrix H . Then, two vectors of F^n are in the same coset of C if and only if they have the same syndrome.

Theorem 32.1 Fundamental Theorem of Galois Theory

Let F be a field of characteristic 0 or a finite field. If E is the splitting field over F for some polynomial in $F[x]$, then the mapping from the set of subfields of E containing F to the set of subgroups of $\text{Gal}(E/F)$ given by $K \rightarrow \text{Gal}(E/K)$ is a one-to-one correspondence. Furthermore, for any subfield K of E containing F ,

- 1. $[E:K] = |\text{Gal}(E/K)|$ and $[K:F] = |\text{Gal}(E/F)| / |\text{Gal}(E/K)|$. [The index of $\text{Gal}(E/K)$ in $\text{Gal}(E/F)$ equals the degree of K over F .]*
- 2. If K is the splitting field of some polynomial in $F[x]$, then $\text{Gal}(E/K)$ is a normal subgroup of $\text{Gal}(E/F)$ and $\text{Gal}(K/F)$ is isomorphic to $\text{Gal}(E/F)/\text{Gal}(E/K)$.*
- 3. $K = E_{\text{Gal}(E/K)}$ [The fixed field of $\text{Gal}(E/K)$ is K .]*
- 4. If H is a subgroup of $\text{Gal}(E/F)$, then $H = \text{Gal}(E/E_H)$. [The automorphism group of E fixing E_H is H .]*

Theorem 32.2 Splitting Field of $x^n - a$

Let F be a field of characteristic 0 and let $a \in F$. If E is the splitting field of $x^n - a$ over F , then the Galois group $\text{Gal}(E/F)$ is solvable.

Theorem 32.3 Factor Group of a Solvable Group Is Solvable

A factor group of a solvable group is solvable.

Theorem 32.4 N and G/N Solvable Implies G Is Solvable

Let N be a normal subgroup of a group G . If both N and G/N are solvable, then G is solvable.

Theorem 32.5 (Galois) Solvable by Radicals Implies Solvable Group

Let F be a field of characteristic 0 and let $f(x) \in F[x]$. Suppose that $f(x)$ splits in $F(a_1, a_2, \dots, a_t)$, where $a_1^{n_1} \in F$ and $a_i^{n_i} \in F(a_1, \dots, a_{i-1})$ for $i = 2, \dots, t$. Let E be the splitting field for $f(x)$ over F in $F(a_1, a_2, \dots, a_t)$. Then the Galois group $\text{Gal}(E/F)$ is solvable.

Theorem 33.1

For every positive integer n , $x^n - 1 = \prod_{d|n} \Phi_d(x)$, where the product runs over all positive divisors d of n .

Theorem 33.2

For every positive integer n , $\Phi_n(x)$ has integer coefficients.

Theorem 33.3 (Gauss)

The cyclotomic polynomials $\Phi_n(x)$ are irreducible over $\mathbb{Z}$.

Theorem 33.4

Let ω be a primitive n th root of unity. Then $\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \approx U(n)$.

Lemma

Let n be a positive integer and let $\omega = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$. Then $\mathbb{Q}(\cos\left(\frac{2\pi}{n}\right)) \subseteq \mathbb{Q}(\omega)$.

Theorem 33.5 (Gauss, 1796)

It is possible to construct the regular n -gon with a straightedge and compass if and only if n has the form $2^k p_1 p_2 \cdots p_t$, where $k \geq 0$ and the p_i 's are distinct primes of the form $2^m + 1$.